REMARKS

The Examiner is thanked for the thorough examination of the present application. The Office Action, however, tentatively rejected all claims 1-20. Specifically, claims 1 and 3-7 stand rejected under 35 U.S.C. 102(a) as allegedly anticipated by PBDM: A Flexible Delegation Model in RBAC (hereinafter PBDM). Claims 2, 8, and 9 stand rejected under 35 U.S.C 103(a) as allegedly unpatentable over PBDM as applied to claim 1 and further in view of RBAC Policies in XML for X.509 Based Privilege Management (hereinafter RBAC). In response, Applicant submits the following remarks.

Fundamental Distinction between Citations and the Present Invention

Applicant respectfully requests reconsideration of the rejections of claims 1-18 of the present application for reasons that will be specifically addressed in following paragraphs. However, before addressing the details of specific rejections, Applicant notes that there are fundamental differences between the disclosure of the cited art and the claimed embodiments.

The present application is generally directed to a delegation method, implemented in a delegation system, comprising the steps of: providing delegation policies as general rules for limiting delegation; receiving a delegation condition and a delegation approval submitted by a grantor for vesting authority of the grantor's role to a grantee, wherein the grantor's role is designated the authority to access a set of data; and determining consequent authority vested to the grantee based on the delegation approval, the delegation condition and the delegation policies.

PBDM discloses that role-based access control is recognized as an efficient access control model for large organizations. Most organizations have some business rules related to access control policy. Delegation of authority is among these rules. RBDM0 and RDM2000 models are recently published models for role-based delegation. They deal with user-to-user delegation. The unit of delegation in them is a role. But, in many situations, users may want to delegate a piece of permission from a role. The cited paper proposes a flexible delegation model named Permission-based Delegation Model (PBDM), which is built on the well-known RBAC96 model. PBDM supports user-to-user and role-to-role delegations with features of multi-step delegation and multi-option revocation. It also supports both role and permission level delegation, which provides great flexibility in authority management. In PBDM, a security administrator specify the permissions that a user (delegator) has authority to delegate to others (delegatee), then the delegator creates one or more temporary delegation roles and assigns delegatees to particular roles. This gives us clear separation of security administration and delegation.

According to RBAC, a role based access control policy template is described for use by privilege management infrastructures where the roles are stored as X.509 Attribute Certificates in an LDAP directory. There is a brief description of the X.509 privilege management model, and how it can be used to implement RBAC. Policies that conform to the template are written in XML, and the template is specified as a DTD. (A future version will specify it as an XML schema). The policy is designed to be used by the PERMIS API, a Java specification for an Access Control Decision Function based on the ISO 10181 Access Control Framework and the Open Group's AZN API.

As described in the present application, the embodiments of the present application provide a dynamic delegation method, which ameliorates problems where the grantor lacks the authority to tailor the vested authority. The dynamic delegation system, according to the claimed embodiments, estimates and verifies delegation based on delegation policies as general rules, which provides identical protection for delegation and data sharing. In addition, delegation conditions defined by grantor increase delegation flexibility, facilitate fitting delegation in aspects of location, hours and data and enhance delegation security to retard delegated authority abuse of the grantee. The dynamic delegation method of the claimed embodiments, as a role-based delegation method, is suitable for implementation in role-based systems. Furthermore, the delegation method of the claimed embodiments enables the grantor to define delegation conditions and, hence, ameliorates the problems of the conventional methods.

The Office Action alleged that the technical features of the inventive embodiments are disclosed in the cited references. However, the citations only relevantly disclose the PBDM theory and RBAC applications.

The embodiments of the present application provide a dynamic delegation method, which ameliorates problems where the grantor lacks the authority to tailor the vested authority by providing delegation policies, receiving a delegation condition and a delegation approval submitted by a grantor for vesting authority of the grantor's role to a grantee, and determining consequent authority vested to the grantee based on the delegation approval, the delegation condition and the delegation policies. The

described technical features of receiving a delegation approval submitted by a grantor for vesting authority of the grantor's role to a grantee and determining consequent authority vested to the grantee based on the delegation approval are not disclosed in the cited references, so the disclosure of the PBDM and RBAC citations are clearly different than that of the inventive embodiments.

Thus, for at least these fundamental reasons, the claimed embodiments are novel and nonobvious in view of the PBDM and RBAC citations.

Rejection of Claim 1

Turning now to the specific rejections, the Office Action rejected independent claim 1 under 35 U.S.C. 102(a) as allegedly anticipated by PBDM. Applicant respectfully requests reconsideration and withdrawal of this rejection for at least the following reasons.

Independent claim 1 recites:

> 1. A delegation method, implemented in a delegation system, comprising the steps of:
> providing delegation policies as general rules for limiting delegation;
> ***receiving a delegation condition and a delegation approval submitted by a grantor for vesting authority of the grantor's role to a grantee***, wherein the grantor's role is designated the authority to access a set of data; and
> ***determining consequent authority vested to the grantee based on the delegation approval***, the delegation condition and the delegation policies.

(*Emphasis added*). Claim 1 patently defines over the cited art for at least the reason that the cited art fails to disclose the features emphasized above.

As reflected above, the embodiment of claim 1 defines a method that receives a delegation condition and a delegation approval submitted by a grantor for vesting

authority of the grantor's role to a grantee and determines consequent authority vested to the grantee based on the delegation approval, the delegation condition and delegation policies. Although the claimed embodiments may utilize some technical features of the PBDM and RBAC citations, the receiving and determining processes are not disclosed therein. Further, the claimed embodiments only apply the PBDM and RBAC concepts for delegation implementation.

For at least the foregoing reasons, claim 1 is novel based on the features of the PBDM citation and should be allowable. As claims 2-9 depend from claim 1, the rejections of these claims should be withdrawn for at least the same reasons.

In addition, with regard to claims 3 and 4, these claims recite:

> 3. The method as claimed in claim 1, wherein the delegation condition comprises a static condition for limiting the vested authority.
> 4. The method as claimed in claim 3, wherein the static condition comprises at least a total time condition, a time condition, a location condition or a function condition.

As reflected above, these claims define that the delegation condition comprises a static condition for limiting the vested authority, and that the static condition comprises at least a total time condition, a time condition, a location condition or a function condition. Relatively, creating a temporary role of the PBDM citation is not directly related to and does not disclose the technical features of clams 3 and 4.

For at least this additional reason, claims 3 and 4 define novel embodiments and the rejections of these claims should be withdrawn..

In addition, with regard to claims 5 and 6, these claims recite:

5. The method as claimed in claim 1, wherein the delegation condition comprises a dynamic condition for limiting the vested authority.

6. The method as claimed in claim 5, wherein the dynamic condition comprises at least a session condition or a group condition.

As reflected above, these claims define that the delegation condition comprises a dynamic condition for limiting the vested authority and the dynamic condition comprises at least a session condition or a group condition.

Relatively, assigning a role to RBAC with group condition change_schedule and role PE of the PBDM citation is not directly related to and does not disclose the technical features of clams 5 and 6. For at least this additional reason, the rejection of claims 5 and 6 should be withdrawn.

In addition, with regard to claim 8, this claim recites:

8. The method as claimed in claim 1, wherein the determining step further comprises the steps of:

determining whether the delegation condition satisfies the delegation policies;

adjusting the delegation condition to the delegation policies when the delegation condition does not satisfy the delegation policies; and

acquiring a consequent delegation condition, where the consequent delegation condition comprises, when the delegation condition does not satisfy the delegation policies, the adjusted delegation condition or, when the delegation condition satisfies the delegation policies, comprises the delegation condition.

As reflected above, claim 8 defines an embodiment that determines whether the delegation condition satisfies the delegation policies, adjusts the delegation condition to the delegation policies when the delegation condition does not satisfy the delegation policies, and acquires a consequent delegation condition, where the consequent

delegation condition comprises, when the delegation condition does not satisfy the delegation policies, the adjusted delegation condition or, when the delegation condition satisfies the delegation policies, comprises the delegation condition.

The RBAC citation discloses similar determining, adjusting, and acquiring operations but does not disclose the other detailed technical features of claim 8. For at least this additional reason, the rejection of claim 8 should be withdrawn.

Rejection of Claims 10-14 and 15-20

The Office Action rejected claims 10-14 and 15-20 on the same basis as claims 1-9. In this regard, the Office Action stated: "Claims 10-15 correspond to the system of claims 1-9 and claims 15-20 correspond to the machine-readable storage medium of claims 1-9 and are hereby rejected with the same logic as the rejection of claims 1-9." Therefore, Applicant submits that these rejections be withdrawn for the reasons set out above in connection with claim 1.

CONCLUSION

In view of the foregoing, it is believed that all pending claims are in proper condition for allowance. If the Examiner believes that a telephone conference would expedite the examination of the above-identified patent application, the Examiner is invited to call the undersigned.

No fee is believed to be due in connection with this amendment and response to Office Action. If, however, any fee is believed to be due, you are hereby authorized to charge any such fee to deposit account No. 20-0778.

Respectfully submitted,

/Daniel R. McClure/

By: _____
Daniel R. McClure
Registration No. 38,962

Thomas, Kayden, Horstemeyer & Risley, LLP
600 Galleria Pkwy, NW
Suite 1500
Atlanta, GA 30339
770-933-9500